What is claimed is:

1. An arithmetic device which performs a multiplication of a multiplicand A and a multiplier B expressed by bit patterns, comprising:

a partial product generation circuit to generate a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

an encoder circuit to encode the multiplier B based on the secondary Booth algorithm, and output a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

a selection circuit to select and output one of the plurality of partial products according to the selection signal; and

an addition circuit to add up partial products equal in number to i output from the selection circuit, and generate a multiplication result, wherein

said arithmetic device has an operation mode in which said encoder circuit outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product

indicating 0 when i is a value other than 0, and said addition circuit generates a two's complement of the multiplicand A from the partial product indicating -A, and outputs the two's complement of the multiplicand A as the multiplication result.

2. An arithmetic device which performs a multiplication of a multiplicand A and a multiplier B expressed by bit patterns, comprising:

a partial product generation circuit to generate a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

an encoder circuit to encode the multiplier B based on the secondary Booth algorithm, and output a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

a selection circuit to select and output one of the plurality of partial products according to the selection signal; and

an addition circuit to add up partial products equal in number to i output from the selection circuit, and generate a multiplication result, wherein

said arithmetic device has an operation mode

in which said encoder circuit outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, and said addition circuit generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs the one's complement of the multiplicand A as the multiplication result.

3. The device according to claim 2, wherein

said encoder circuit outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0 regardless of a value of the multiplier B in the operation mode.

4. The device according to claim 2, wherein

said encoder circuit outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0 and when 0 is input as the multiplier B in the operation mode.

5. An arithmetic device which performs a

multiplication-addition by performing a multiplication of a multiplicand A and a multiplier B expressed by bit patterns and then adding up a multiplication result, a number C, and a number D expressed by bit patterns, comprising:

a partial product generation circuit to generate a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

an encoder circuit to encode the multiplier B based on the secondary Booth algorithm, and output a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

a selection circuit to select and output one of the plurality of partial products according to the selection signal; and

an addition circuit to add up partial products equal in number to i output from said selection circuit, the number C, and the number D, and generating a multiplication-addition result, wherein

said arithmetic device has an operation mode in which said encoder circuit outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection

signal for selection of a partial product indicating 0 when i is a value other than 0, and said addition circuit generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs a result of adding up the one's complement of the multiplicand A, the number C, and the number D as the multiplication-addition result.

6. An arithmetic device which performs an operation of subtracting an integer N containing g k-bit blocks from an integer Y containing g+1 k-bit blocks by performing a multiplication of a multiplicand A and a multiplier B expressed by k-bit bit patterns and then adding up a multiplication result, a number C, and a number D expressed by k-bit bit patterns, comprising:

a partial product generation circuit to generate a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

an encoder circuit to encode the multiplier B based on the secondary Booth algorithm, and output a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

a selection circuit to select and output one of the plurality of partial products according to the selection signal;

an addition circuit to add up partial products equal in number to i output from said selection circuit, the number C, and the number D, and generate a 2k-bit multiplication-addition result; and

an inverter to invert a part of bits of the multiplication-addition result, wherein

said partial product generation circuit uses a j-th block n_j of the integer N as the multiplicand A, said encoder circuit outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, said addition circuit generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs a result of adding up the one's complement of the multiplicand A, the number C, and the number D as a multiplication-addition result of a j-th block using a carry from a multiplication-addition of a (j-1)th block as the number C and a j-th block y_j of the integer Y as the number D, and said inverter

inverts a part of bits of the multiplication-addition result of the j-th block, and generates a carry to a multiplication-addition of a (j+1)th block.

7. An arithmetic device which divides integers I and J and a modulus N of residue arithmetic expressed by bit patterns, into g k-bit blocks, respectively and performs multiple precision arithmetic for Montgomery multiplication residue arithmetic of $Y = IJ2^{-kg} \bmod N$, comprising:

a first selection circuit to select and output one of a plurality of given values for each of a k-bit multiplicand A, multiplier B, number C, and number D;

a partial product generation circuit to generate a plurality of partial products in a secondary Booth algorithm from the multiplicand A output from said first selection circuit;

an encoder circuit to encode the multiplier B based on the secondary Booth algorithm, and output a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B output from said first selection circuit;

a second selection circuit to select and output one of the plurality of partial products according to the selection signal;

an addition circuit to add up partial products equal in number to i output from said second selection circuit, the number C, and the number D output from said first selection circuit, and to generate a 2k-bit multiplication-addition result; and

an inverter to invert a part of bits of the multiplication-addition result, wherein

said arithmetic device has an operation mode in which said first selection circuit selects a j-th block n_j of the integer N as the multiplicand A, selects a carry from a multiplication-addition of a (j-1)th block as the number C, and selects a j-th block y_j as the number D, said encoder circuit outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, said addition circuit generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs a result of adding up the one's complement of the

multiplicand A, the number C, and the number D as a multiplication-addition result of a j-th block, and said inverter inverts a part of bits of the multiplication-addition result of the j-th block, and generates a carry to a multiplication-addition of a (j+1)th block.

8. An arithmetic device which performs a multiplication of a multiplicand A and a multiplier B expressed by bit patterns, comprising:

partial product generation means for generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoder means for encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

selection means for selecting and outputting one of the plurality of partial products according to the selection signal; and

addition means for adding up partial products equal in number to i output from said selection means, and generating a multiplication result, wherein

said arithmetic device has an operation mode in which said encoder means outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, and said addition means generates a two's complement of the multiplicand A from the partial product indicating -A, and outputs the two's complement of the multiplicand A as the multiplication result.

9. An arithmetic device which performs a multiplication of a multiplicand A and a multiplier B expressed by bit patterns, comprising:

partial product generation means for generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoder means for encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

selection means for selecting and outputting one of the plurality of partial products according to the selection signal; and

addition means for adding up partial products equal in number to i output from said selection means, and generating a multiplication result, wherein

said arithmetic device has an operation mode in which said encoder means outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, and said addition means generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs the one's complement of the multiplicand A as the multiplication result.

10. An arithmetic device which performs a multiplication-addition by performing a multiplication of a multiplicand A and a multiplier B expressed by bit patterns and then adding up a multiplication result, a number C, and a number D expressed by bit patterns, comprising:

partial product generation means for generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoder means for encoding the multiplier B

based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

selection means for selecting and outputting one of the plurality of partial products according to the selection signal; and

addition means for adding up partial products equal in number to i output from the selection means, the number C, and the number D, and generating a multiplication-addition result, wherein

said arithmetic device has an operation mode in which said encoder means outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, and said addition means generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs a result of adding up the one's complement of the multiplicand A, the number C, and the number D as the multiplication-addition result.

11. An arithmetic device which performs an operation of subtracting an integer N containing g k-bit blocks from an integer Y containing g+1 k-bit blocks by performing a multiplication of a multiplicand A and a multiplier B expressed by k-bit bit patterns and then adding up a multiplication result, a number C, and a number D expressed by k-bit bit patterns, comprising:

partial product generation means for generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoder means for encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B;

selection means for selecting and outputting one of the plurality of partial products according to the selection signal;

addition means for adding up partial products equal in number to i output from said selection means, the number C, and the number D, and generating a 2k-bit multiplication-addition result; and

inverter means for inverting a part of bits of

the multiplication-addition result, wherein

said partial product generation means uses a j-th block n_j of the integer N as the multiplicand A, said encoder means outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, said addition means generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs a result of adding up the one's complement of the multiplicand A, the number C, and the number D as a multiplication-addition result of a j-th block using a carry from a multiplication-addition of a (j-1)th block as the number C and a j-th block y_j of the integer Y as the number D, and said inverter means inverts a part of bits of the multiplication-addition result of the j-th block, and generates a carry to a multiplication-addition of a (j+1)th block.

12. An arithmetic device which divides integers I and J and a modulus N of residue arithmetic expressed by bit patterns, into g k-bit blocks, respectively and performs multiple precision

arithmetic for Montgomery multiplication residue arithmetic of $Y = IJ2^{-kg} \bmod N$, comprising:

first selection means for selecting and outputting one of a plurality of given values for each of a k-bit multiplicand A, multiplier B, number C, and number D;

partial product generation means for generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A output from said first selection means;

encoder means for encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B output from said first selection means;

second selection means for selecting and outputting one of the plurality of partial products according to the selection signal;

addition means for adding up partial products equal in number to i output from said second selection means, the number C, and the number D output from said first selection means, and generating a 2k-bit multiplication-addition result; and

inverter means for inverting a part of bits of the multiplication-addition result, wherein

said arithmetic device has an operation mode in which said first selection means selects a j-th block n_j of the integer N as the multiplicand A, selects a carry from a multiplication-addition of a (j-1)th block as the number C, and selects a j-th block y_j as the number D, said encoder means outputs a selection signal for selection of a partial product indicating -A when i is 0, and outputs a selection signal for selection of a partial product indicating 0 when i is a value other than 0, said addition means generates a one's complement of the multiplicand A from the partial product indicating -A, and outputs a result of adding up the one's complement of the multiplicand A, the number C, and the number D as a multiplication-addition result of a j-th block, and said inverter means inverts a part of bits of the multiplication-addition result of the j-th block, and generates a carry to a multiplication-addition of a (j+1)th block.

13. An arithmetic method for performing a multiplication of a multiplicand A and a multiplier

B expressed by bit patterns, comprising the steps of:

generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B, wherein outputting a selection signal for selection of a partial product indicating -A when i is 0, and outputting a selection signal for selection of a partial product indicating 0 when i is a value other than 0;

selecting and outputting one of the plurality of partial products according to the selection signal; and

adding up partial products equal in number to i output by said selecting operation, and generating a multiplication result, wherein generating a two's complement of the multiplicand A from the partial product indicating -A, and outputting the two's complement of the multiplicand A as the multiplication result.

14. An arithmetic method for performing a multiplication of a multiplicand A and a multiplier B expressed by bit patterns, comprising the steps of:

generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B, wherein outputting a selection signal for selection of a partial product indicating -A when i is 0, and outputting a selection signal for selection of a partial product indicating 0 when i is a value other than 0;

selecting and outputting one of the plurality of partial products according to the selection signal; and

adding up partial products equal in number to i output by said selecting operation, and generating a multiplication result, wherein generating a one's complement of the multiplicand A from the partial product indicating -A, and outputting the one's complement of the multiplicand

A as the multiplication result.

15. An arithmetic method for performing a multiplication-addition by performing a multiplication of a multiplicand A and a multiplier B expressed by bit patterns and then adding up a multiplication result, a number C, and a number D expressed by bit patterns, comprising the steps of:

generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A;

encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B, wherein outputting a selection signal for selection of a partial product indicating -A when i is 0, and outputting a selection signal for selection of a partial product indicating 0 when i is a value other than 0;

selecting and outputting one of the plurality of partial products according to the selection signal; and

adding up partial products equal in number to i output by said selecting operation, the number C,

and the number D, and generating a multiplication-addition result, wherein generating a one's complement of the multiplicand A from the partial product indicating -A, and outputting a result of adding up the one's complement of the multiplicand A, the number C, and the number D as the multiplication-addition result.

16. An arithmetic method for performing an operation of subtracting an integer N containing g k-bit blocks from an integer Y containing g+1 k-bit blocks by performing a multiplication of a multiplicand A and a multiplier B expressed by k-bit bit patterns and then adding up a multiplication result, a number C, and a number D expressed by k-bit bit patterns, comprising the steps of:

generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A by using a j-th block n_j of the integer N as the multiplicand A;

encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and

b_{2i-1} of the multiplier B, wherein outputting a selection signal for selection of a partial product indicating -A when i is 0, and outputting a selection signal for selection of a partial product indicating 0 when i is a value other than 0;

selecting and outputting one of the plurality of partial products according to the selection signal;

adding up partial products equal in number to i output by said selecting operation, the number C, and the number D, and generating a 2k-bit multiplication-addition result, wherein generating a one's complement of the multiplicand A from the partial product indicating -A, and outputting a result of adding up the one's complement of the multiplicand A, the number C, and the number D as a multiplication-addition result of a j-th block using a carry from a multiplication-addition of a (j-1)th block as the number C and a j-th block y_j of the integer Y as the number D; and

inverting a part of bits of the multiplication-addition result, wherein inverting a part of bits of the multiplication-addition result of the j-th block, and generating a carry to a multiplication-addition of a (j+1)th block.

17. An arithmetic method for dividing integers I and J and a modulus N of residue arithmetic expressed by bit patterns, into g k-bit blocks, respectively and performing multiple precision arithmetic for Montgomery multiplication residue arithmetic of $Y = IJ2^{-kg} \bmod N$, comprising the steps of:

first selecting and outputting one of a plurality of given values for each of a k-bit multiplicand A, multiplier B, number C, and number D, wherein selecting a j-th block n_j of the integer N as the multiplicand A, selecting a carry from a multiplication-addition of a (j-1)th block as the number C, and selecting a j-th block y_j as the number D;

generating a plurality of partial products in a secondary Booth algorithm from the multiplicand A output by said first selecting operation;

encoding the multiplier B based on the secondary Booth algorithm, and outputting a selection signal depending on a value of i specifying three consecutive bits b_{2i+1}, b_{2i}, and b_{2i-1} of the multiplier B output by said first selecting operation, wherein outputting a selection

signal for selection of a partial product indicating -A when i is 0, and outputting a selection signal for selection of a partial product indicating 0 when i is a value other than 0;

second selecting and outputting one of the plurality of partial products according to the selection signal;

adding up partial products equal in number to i output by said second selecting operation, the number C, and the number D output by said first selecting operation, and generating a 2k-bit multiplication-addition result, wherein generating a one's complement of the multiplicand A from the partial product indicating -A, and outputting a result of adding up the one's complement of the multiplicand A, the number C, and the number D as a multiplication-addition result of a j-th block; and

inverting a part of bits of the multiplication-addition result, wherein inverting a part of bits of the multiplication-addition result of the j-th block, and generating a carry to a multiplication-addition of a (j+1)th block.